REMARKS

The examiner is thanked for the performance of a thorough search.

By this amendment, Claims 39-43 are added, and no claims are amended or canceled. Hence, Claims 1, 3-11, and 26-43 are pending in the application.

The amendments to the claims as indicated herein do not add any new matter to this application and raise no new issues. In fact, Claims 39-43 recite the same subject matter as apparatus Claims 29-33 and apparatus Claims 34-38, except Claims 39-43 are computer-readable storage medium claims.

Each issue raised in the Office Action mailed June 12, 2008 is addressed hereinafter.

I. SUMMARY OF THE INTERVIEW

The Examiner is thanked for the telephone interview held on September 4, 2008. The Examiner and representatives of the Applicants reached an agreement that Claim 1 is patentable over U.S. Patent No. 6,073,178 issued to Wong et al. ("*Wong*").

II. ISSUES RELATING TO THE CITED ART

Claims 1, 3, 6, 7, 9-11, 26-30, 32-35, and 37-38 stand rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by *Wong*. This rejection is respectfully traversed.

Claims 4 and 5 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Wong* in view of U.S. Patent Publication No. 2002/0026573 to Park ("*Park*"). This rejection is respectfully traversed.

Claims 8, 31, and 36 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Wong* in view of U.S. Patent No. 6,782,422 issued to Bahl et al. ("*Bahl*"). This rejection is respectfully traversed.

A. CLAIM 1

Claim 1 recites:

> A method of assigning a network address to a host based on **authentication for a physical connection between the host and an intermediate device**, the method comprising the computer-implemented steps of:
> **receiving, at a router hosting an authenticator process for the host, from a first server that provides authentication and authorization, in response to a request for authentication for the physical connection, first data indicating at least some of authentication and authorization information**;
> receiving, at a DHCP relay agent process of the router, from the host, a DHCP discovery message for discovering a logical network address for the host;
> generating at the DHCP relay agent process a second message that comprises the DHCP discovery message and the first data; and
> sending the second message from the DHCP relay agent process to a DHCP server that provides the logical network address for the host;
> wherein generating the second message further comprises sending a third message, from the authenticator process to the relay agent process, that contains at least some of the authentication and authorization information based on the first data. (emphasis added)

Wong fails to teach or suggest numerous features of Claim 1. *Wong* is directed to solving a problem that is different than a problem solved by Claim 1. *Wong* is directed to a method for assigning IP addresses that discourages IP address forging (col. 2, lines 39-41). *Wong* accomplishes this by having a router 106 (between a client system 102 and a DHCP server 106) include a "trusted" identifier to a DHCP request from the client system 102. The DHCP server assigns an IP address to the client system and sends a DHCPACK message (which includes the trusted identifier) to the client system 102. Router 106 intercepts the DCHPACK message and, before forwarding the DHCPACK message to client system 102, makes an association between the IP address and the trusted identifier. Col. 3, lines 12-21 of *Wong* then states:

> When the router [106] receives a packet directed at a learned IP address, it forwards the packet to the modem that is associated with the learned IP address. This action prevents client systems from usurping IP addresses to gain illicit access to IP packets. Additionally, when the router [106] receives a packet from a modem, it compares the source address included in the packet with the IP

> addresses that are associated with that modem. If the packet does not originate from an IP address that the router [106] recognizes as being associated with the sending modem, the packet is discarded.

In contrast, Claim 1 prevents a DHCP server from having to re-authenticate a host, i.e., a host that has already been authenticated before requesting a logical network address.

1. Wong *fails to teach or suggest the recited first data*

The Office Action cites col. 8, lines 53-67 of *Wong* for allegedly disclosing the step of "receiving, at a router hosting an authenticator process for the host, from a first server that provides authentication and authorization, in response to a request for authentication for the physical connection, first data indicating at least some of authentication and authorization information," as recited in Claim 1. This is incorrect. That portion of *Wong* merely states:

> If a downstream packet is detected in step 804, execution of method 800 continues at step 806 where the router 106 extracts the packet's destination address. Using this destination address, the router 106, in step 808 "looks up" the trusted identifier of the client system 102 that is associated with the destination address of the received packet (this association is formed by the router 106 during execution of method 600). In step 810, a test is performed to ascertain whether a trusted identifier was actually located in step 808. If a trusted identifier was located in step 808, execution of method 800 continues at step 812 where the router 106 forwards the received packet to client system associated with the trusted identifier. In the alternative, if no trusted identifier is associated with the destination address of the packet, the router 106 discards the packet in step 814.

The Office Action appears to equate (1) router 106 of *Wong* with the router of Claim 1 and (2) the "trusted" identifier of *Wong* with the authentication and authorization (AA) information of Claim 1. This is incorrect for at least two reasons. First, the "trusted" identifier is an identifier that router 106 assigns to an IP address of a client system. The trusted identifier is <u>not</u> received at router 106 <u>from a **server** that provides AA information</u>, as Claim 1 requires. The only processes referred to in the cited portions of *Wong* are client system 102 (i.e., the alleged "host"), router 106 (i.e., the alleged "router"), and DHCP server 114 (i.e., the alleged "DHCP server"). Second, the trust identifier of *Wong* is not received in response to a request for authentication for a physical connection, as Claim 1 requires.

Based on the foregoing, *Wong* fails to teach or suggest all the limitations of Claim 1. Therefore, Claim 1 is patentable over *Wong*. Reconsideration and withdrawal of the rejection of Claim 1 under 35 U.S.C. § 102(b) is therefore respectfully requested.

B. CLAIMS 26-28

Each of the features discussed above for Claim 1 is present in independent Claims 26-28. Therefore, Claims 26-28 are patentable for at least those reasons that Claim 1 is patentable as set forth above.

C. CLAIMS 3-8, 10-11, AND 29-43

Each of the features discussed above for Claim 1 is present, by dependency, in Claims 3-8, 10-11, and 29-43. Because each of the dependant claims includes the limitations of claims upon which they depend, the dependant claims are patentable for at least those reasons the claims upon which the dependant claims depend are patentable.

III. CONCLUSIONS & MISCELLANEOUS

For the reasons set forth above, all of the pending claims are now in condition for allowance. The Examiner is respectfully requested to contact the undersigned by telephone relating to any issue that would advance examination of the present application.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Dated: September 5, 2008

/DanielDLedesma#57181/
Daniel D. Ledesma
Reg. No. 57,181

2055 Gateway Place Suite 550
San Jose, California 95110-1083
Telephone No.: (408) 414-1080 ext. 229
Facsimile No.: (408) 414-1076